UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/598,777	06/16/2000	Steven H. McCown	00-022-MIS	5604

7590 10/23/2002

Wayne P Bailey
Storage Technology Corporation
One StorageTek Drive
Louisville, CO 80028-4309

EXAMINER
LE, DAVID Q

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 10/23/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/598,777	MCCOWN ET AL.	
	Examiner	Art Unit	
	David Q Le	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-40 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-40 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1-40** are rejected under 35 U.S.C. 103(a) as being unpatentable over ***Vizcaino*** in view of ***Taylor*** and further in view of ***Berger et al.***, US Patents Nos ***5,317,636***, ***5,530,232*** and ***5,850,446*** respectively.

Vizcaino discloses a method and apparatus for improving the security of credit card transactions involving "smart cards" equipped with a processor and storage memory, communicating with a verification computer via a digital network. When used, the cards produce a transaction verification number that is encrypted and then transmitted to the remote verification computer. The verification computer decrypts this number, retrieves the card owner's account information from its databases, computes a corresponding verification number, and compares the two numbers thus produced. If there's a match, the transaction is authorized and executed, and the card is updated with adjusted information (Abstract, Description, Figs 1-6).

Taylor discloses a multi-application card system that enables and manages electronic transactions. The system uses smart cards or credit cards that are read by card readers at point-of-sale (POS) terminals (Fig 2-3); the customer's information, merchant information, and transaction specific data are transmitted via data link to a processing center where the data is authenticated and the transaction authorized and executed, customer and merchant accounts are debited/credited accordingly, confirmation and receipts are returned to the point-of-sale, and updated data gets written onto the smart cards' storage memory (Fig 4).

Berger discloses a system for securing data transmissions within a payment system between computers operated by a buyer, merchant, and central processing authority ("payment gateway"). The payment gateway system evaluates a payment request and returns authorization of the payment to the merchant, after which the transaction is concluded, processed by the payment gateway, and customer and merchant's accounts are updated accordingly (Abstract; Fig 1-5).

As per **claims 1-2, 5-6**:

Both *Vizcaino* (Fig 6, related description) and *Taylor* (Figs 2-4, related description) require that the customer's card forward unique customer information (Applicant's "unique client information") and transaction information (product or service requested) to the POS or card reader, for the purpose of further transmitting this data to an authorization/payment center. Both *Vizcaino* (Figs 2A-3, 6, related description; Col 5, lines 14-34) and *Taylor* (Col 6, lines 50-51) teach that this data may be encrypted by any convenient encryption method prior to transmission.

Berger (Figs 2-5, related description; Cols 13-16) describes how a "basic authorization request" (Fig 5A, Col 16, lines 2-15) consisting of customer information, merchandise/service information, and customer passwords/authentication data (i.e.PINs and/or customer master key), may be created between merchant and customer. This information is communicated by the customer to the merchant using cryptographic methods well known in the art (Col 14, line 52 – Col 15, line 1). Berger further describes how the merchant system then creates a "combined authorization request" (basic authorization request + merchant information/encryption keys/certificates) (Fig 4, related description), encrypts it, and hashes it to produce a "message digest" prior to transmitting this digest to an authorization/payment center (Col 15, line 65 – Col 16, line 41; Figs 4-5F).

Vizcaino and *Taylor* teach that smart cards may be manufactured to store and interactively provide widely variable and unique customer data that can be provided to a merchant system for the purpose of authorizing and authenticating a transaction. *Berger* teaches a method similar to Applicant's for further securing said customer/transaction information combined with merchant information prior to transmission to an authorization/payment center.

The above references disclose the limitations of claim 1 except for having the smart card itself combining all the required authorization data for a transaction, encrypting this data and hashing it, prior to transmitting the resulting "digest" to a merchant. However, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement this method of securing the data onto the smart card itself prior to transmission to the merchant's system, for the purpose of further insulating sensitive customer information from any unauthorized capture, in view of the processing capability already available on the card. It has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse, 86 USPQ 70.*

1.A method for securing a transaction ... used for transacting with a third party.
2.The method recited in claim 1 ... hashing the unique requestor information.
5.The method recited in claim 1 ... is performed by a smart card.
6.The method recited in claim 1 ... retrieving the unique client information.

As per **claim 3**:

Taylor discloses that transactions effected by a smart card may be paid from different customer accounts (i.e. Visa, Mastercard, Amex, etc.) (Fig 1). This would mean that the merchant would have to communicate to the smart card which among those credit card issuers the merchant has a corresponding account with, causing the smart card to access the proper master key for that particular credit card issuer.

3.The method recited in claim 1 ... used to access the master key.

As per **claims 4, 7-11**:

Vizcaino discloses the use of a unique transaction number (Fig 2A, related description) in creating an authorization request. *Vizcaino* also discloses that such unique transaction number may be one of a plurality (or a range) of numbers provided to the client by the authorizing party.

4. The method recited in claim ... to the client by the third party.
7. The method recited in claim 1 ... a purchase initiated by the client.
8. A method for securing a ... client information to the requestor.
9. The method recited in claim 8 ... to the client by the credit card issuer.
10. The method recited in claim 8 ... passing the information to the merchant.

11. A method for securing a transaction ... to a credit card issuer.

As per **claims 12-30, 32-40**:

All three references cited feature authorizing/payment processing centers where each transaction is sent for authorization, capture, and where merchant and customer accounts will be updated. Once authorization is obtained, it is communicated back to the merchant's system, so that the transaction maybe completed, receipts printed, and/or customer card updated electronically. *Vizcaino* uses a comparison between a unique transaction number generated by the customer's card and a corresponding number generated by the authorizing center to determine authorization (Fig 6, related description). *Berger* provides detailed descriptions on various methods for said authorization, processing, and confirmation (Figs 6-12, related description). It would have been obvious to one ordinarily skilled in the art at the time the invention was made to combine the features described in the cited references to create a system meeting all the limitations of the claims listed below. This would have been done to provide a secure, reliable, and effective payment system utilizing credit, debit, and smart cards, usable at merchant POS terminals as well as on a network such as the Internet.

12. The method recited in claim 11 ... receiving a response from the credit card issuer.
13. A method for securing ... with the digest from the requestor.
14. The method recited in claim ... the unique requestor information.
15. The method recited in claim 13 ... by the third party.
16. The method recited in claim 15 ... number contained in the unique client information.
17. The method recited in claim 13 ... performed by a smart card.
18. The method recited in claim 13 ...accessing the master key.
19. The method recited in claim 13 ... purchase initiated by the client.
20. A method for securing a transaction ... authorization digest with the billing digest.
21. A method for securing a transaction ... and the master key.
22. A smart card for conducting ... account information to a requestor.
23. A system for conducting secure transactions ... with a third party.
25. The system recited in claim 24 ... unique requestor information.
26. The system recited in claim 24 ...access the master key.
27. The system recited in claim 24 ...to the client by the third party.
28. The system recited in claim 24 ...performed by a smart card.
29. The system recited in claim 24 ... the unique client information.
30. The system recited in claim 24 ... transaction initiated by the client.
32. A system for securing a transaction ... digest from the requestor.
33. The system recited in claim 32 ... hashing the unique requestor information.
34. The system recited in claim 32 ... by the third party.
35. The system recited in claim ... the unique client information.
36. The system recited in claim 32 ... performed by a smart card.
37. The system recited in claim 32 ... prior accessing the master key.
38. The system recited in claim 32 ... initiated by the client.
39. A computer program product ... for transacting with a third party.
40. A computer program product ... information to the requestor.

As per **claim 31**:

Taylor discloses that biometric identifiers (voice, fingerprint, photo) may be incorporated on smart cards to further authenticate and authorize legitimate users of said cards (Fig 4, related description). It would have been obvious to one ordinarily skilled in the art

to have added this feature to any embodiment of a payment system based on said cards should the need present itself for this level of security.

31. The system recited in claim 24 ... of a client's fingerprint.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Q Le whose telephone number is 703-305-4567. The examiner can normally be reached on 8:30am-5: 30pm Mo-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on 703-305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-7687 for regular communications and 703-305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

DQL
October 17, 2002

JAMES P TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600